Amendment to the Claims

1.(currently amended) A user interface for displaying processed and analyzed network traffic data to an end user, comprising:

a system dashboard kept up to date with current monitoring information comprising network traffic data from a monitored network, said dashboard comprising:

a network status console area;

a network events viewing area; and

a trend viewing area.

2. (original) The user interface of Claim 1, wherein said network status console area further comprises:

an alerts area comprising a FIFO queue of critical alerts; and

a health monitor area showing a percentage of network traffic that does not violate current traffic and over a predetermined amount of time.

3. (original) The user interface of Claim 1, further comprising:

a tear off status console window for said end user to keep console window open on a desktop to monitor network status.

4. (original) The user interface of Claim 1, using a web page paradigm.

5. (original) The user interface of Claim 2, wherein said user alerts are updated on a real-time basis.

6. (original) The user interface of Claim 2, wherein any of said user alerts links to corresponding alert details information.

7. (original) The user interface of Claim 2, wherein the underlying traffic data of said health monitor is updated automatically at a regular interval.

8. (original) The user interface of Claim 2, wherein severity alerts levels are distinguished by color codes.

9. (original) The user interface of Claim 1, wherein said network events viewing area further comprises links to any of the following:

summary information;
information on all events; and
policy history information;
wherein a configurable time period is set.

10. (original) The user interface of Claim 9, wherein said configurable time period comprises any of:

a user selected date and time range;
last two hours;
today;
last 24 hours;
yesterday;
last seven days;
this month;
last month; and
last three months.

11. (original) The user interface of Claim 1, further comprising any of:

conformance events summary information containing a count of violations for each rule/disposition pair;

violator events summary information containing a count of the number of violations for each violating ip-address; and

target events summary information containing a count of the number of violations for each top destination ip-address.

12. (original) The user interface of Claim 11, wherein event summary information links to network event details information containing details on events making up said count.

13. (original) The user interface of Claim 1, wherein user defined and configurable query and report settings are stored.

14. (original) The user interface of Claim 1, wherein said trend viewing area further comprises links to network events summary information.

15. (original) The user interface of Claim 1, wherein said trend viewing area further comprises a QuickWeek section, containing any of:

a predetermined number of most frequent rule/disposition combinations during a past predetermined number of days;

a predetermined number of most frequent violator ip-addresses versus count during said past predetermined number of days; and

a predetermined number of most frequent target ip-addresses versus count during said past predetermined number of days.

16. (original) The user interface of Claim 1, wherein the trend viewing area is user customizable.

17. (original) The user interface of Claim 1, further comprising embeddable trend charts into details information, said trend over a time range dynamically configurable by said end user.

18. (original) The user interface of Claim 17, wherein said trend charts comprise any of:

policy effectiveness;
number of policy changes over time;
event summary;
network event details; and
all conformance counts.

19. (original) The user interface of Claim 12, wherein said network event details information further comprises any of:

monitoring point;
disposition name;
rule name;
disposition code;
severity;
source ip-address;

source port;
destination ip-address;
destination port;
ip protocol;
event time; and
application data.

20. (original) The user interface of Claim 19, wherein said application data comprises any of, but not limited to:
ICMP action code;
HTTP -URL;
FTP-Filename;
SSL – Ciphersuite, Issuer and Subject's certificate CommonName, Certificate Status;
SSH– Authentication handshake status; and
application status code.

21. (original) The user interface of Claim 1, further comprising protocol event details information in context of a particular network event to a database from which said information is retrieved on an as-needed basis.

22. (original) The user interface of Claim 21, wherein said protocol event details information further comprises data from attributes.

23. (original) The user interface of Claim 22, wherein said data attributes comprise any of, but not limited to:
initiator credential name;
target credential name;
rule name for said protocol event; and
disposition name for said protocol event.

24. (original) The user interface of Claim 1, further comprising alert event details information, said information comprising any of:
details of network event that caused alert;
rule and disposition name that triggered alert;
log comment from corresponding disposition;

time at which alert was generated;
initiator ip address of the corresponding non-conformant traffic;
target ip address of the corresponding non-conformant traffic;
an icon that links to the network event details page describing the non-conformant network event; and
checkbox to clear alert;

25. (original) The user interface of Claim 1, further comprising a policy update information area showing each time a new policy is installed, said information comprising:
date of policy information;
description of policy; and
link to English representation of said newly installed policy.

26. (original) The user interface of Claim 2, further comprising means for each of said alerts to generate an alert email, said alert email comprising any of, but not limited to:
time said alert occurred;
rule and disposition name that triggered alert;
log description from said corresponding disposition;
initiator ip address of corresponding non-conformant traffic;
target ip address of corresponding non-conformant traffic; and
a link to network event detail, said detail describing said non-conformant network event.

27. (original) The user interface of Claim 26, further comprising a customer information area allowing said end user to configure a list of email addresses to receive said alert email.

28. (original) The user interface of Claim 1, further comprising means for ad-hoc querying by said end user.

29. (original) The user interface of Claim 28, wherein means for ad-hoc querying further comprises filtering results by, but not limited to any or all of:

protocol of rule name;
policy rule name;
regular expression within rule name;
disposition name of violation;
regular expression within disposition name;
source ip-address;
regular expression with source ip-address;
target ip-address;
regular expression within target ip-address;
target port; and
regular expression within target port.

30. (original) The user interface of Claim 28, wherein means for ad-hoc querying further comprises an advanced search feature.

31. (original) The user interface of Claim 30, wherein said advanced search feature is implemented using a dialog box.

32. (original) The user interface of Claim 1, further comprising informational aids, said information aids comprising any of:
English language representation of policy;
rule and disposition descriptions; and
copyright information.

33. (original) The user interface of Claim 32, wherein said informational aids are linked to by said end user when said end user places a cursor over an appropriate field thereby displaying a tooltip of corresponding descriptions of said fields.

34. (original) The user interface of Claim 33, wherein said descriptions are any of but not limited to:
rule descriptions;
disposition descriptions; and
Resolved DNS names for ip-addresses; and
TCP and UDP service names.

35. (original) The user interface of Claim 33, wherein said informational aids further comprise any of:

context sensitive help;

36. (original) The user interface of Claim 1, further comprising a link to generate a printer friendly printed page.

37. (original) The user interface of Claim 1, further comprising displaying time information in a predetermined time zone.